11. How can you prioritize and remediate vulnerabilities based on scan results?

🔍 Prioritizing & Remediating Vulnerabilities from Nessus Scan Results

When Nessus completes a scan, it provides a **list of detected vulnerabilities**, but not all require **immediate action**. To efficiently **secure your system**, you must prioritize and remediate vulnerabilities based on their **severity, exploitability, and business impact**.

📌 Step 1: Understand Vulnerability Severity & Risk

Nessus assigns a **severity level** based on the **Common Vulnerability Scoring System (CVSS)**:

Severity	CVSS Score	Risk Level	Action Required?
🔴 **Critical**	9.0 - 10.0	Actively exploitable, high impact	**Immediate remediation**
🟠 **High**	7.0 - 8.9	Exploitable with serious consequences	**Fix ASAP**
🟡 **Medium**	4.0 - 6.9	Potentially exploitable	**Fix when possible**
🔵 **Low**	0.1 - 3.9	Low risk, hard to exploit	**Monitor, plan remediation**
⚪ **Informational**	0.0	No security impact	**No action needed**

✓ **Focus on Critical** & **High** vulnerabilities first.
✓ **Medium & Low** risks should be fixed **based on exploitability** and **business impact**.

📊 Step 2: Categorize Vulnerabilities for Prioritization

1️⃣ Immediate Threats (Highest Priority)

✅ **Characteristics:**

- **Publicly available exploits**
- **Remote Code Execution (RCE) vulnerabilities**
- **Privilege escalation flaws**

- **Active exploitation in the wild**
- **Affects critical systems (e.g., databases, authentication servers, financial systems)**

🛠️ **Action: Patch immediately** or apply **temporary mitigations** (e.g., firewall rules).

2️⃣ High-Risk Vulnerabilities (Fix ASAP)

✅ **Characteristics:**

- **Denial of Service (DoS) risks**
- **Authentication bypass vulnerabilities**
- **SQL Injection (SQLi), Cross-Site Scripting (XSS)**
- **Misconfigurations exposing sensitive data**

🛠️ **Action:**

- **Patch** within a defined timeframe.
- **Enhance security controls** (e.g., Web Application Firewall for XSS).

3️⃣ Medium & Low-Risk Vulnerabilities (Fix When Feasible)

✅ **Characteristics:**

- **Local privilege escalation (requires user interaction)**
- **Brute-force vulnerabilities** (e.g., weak SSH configurations)
- **Unpatched services running internally**

🛠️ **Action:**

- **Fix in the next patch cycle** if no active exploit exists.
- **Monitor & track for future updates**.

4️⃣ False Positives (Ignore or Reassess)

✅ **Characteristics:**

- Vulnerability exists **only in a theoretical attack scenario**.
- Security layers **already mitigate the risk** (e.g., IDS, firewalls).

🛠️ **Action:**

- **Verify manually** before excluding from future scans.
- If a false positive, mark it as **"accepted risk"** in Nessus.

🔧 Step 3: Remediation Strategies

🔹 1. Patch Management

- **Apply vendor patches** as soon as possible (especially for Critical & High risks).
- Schedule updates during maintenance windows.

🔹 2. Network Segmentation & Firewall Rules

- Isolate **vulnerable systems** until patches are applied.
- Block **unnecessary open ports**.

🔹 3. Configuration Hardening

- Disable **unnecessary services**.
- Enforce **stronger authentication**.

🔹 4. Monitor & Verify Fixes

- **Re-scan after applying fixes** to ensure vulnerabilities are resolved.
- **Monitor logs** for suspicious activity.

🚀 Final Thoughts

✓ Prioritize Critical & High vulnerabilities first.
✓ Use CVSS scores, exploitability, and business impact to decide remediation urgency.
✓ Apply patches, firewall rules, and configuration changes as needed.
✓ Always verify fixes with follow-up scans.